



# FortiSwitch Release Notes

**Version 3.6.10**

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



November 8, 2019

FortiSwitch 3.6.10 Release Notes

11-3610-565717-20191108

# TABLE OF CONTENTS

<b>Change log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
Supported models	5
What's new in 3.6.10	5
<b>Special notices</b>	<b>6</b>
Supported features for FortiSwitchOS 3.6.10	6
<b>Upgrade information</b>	<b>11</b>
Cooperative Security Fabric upgrade	11
<b>Product integration and support</b>	<b>12</b>
FortiSwitch 3.6.10 support	12
<b>Resolved issues</b>	<b>13</b>
<b>Known issues</b>	<b>14</b>

## Change log

Date	Change Description
July 12, 2019	Initial document release for FortiSwitchOS 3.6.10
November 8, 2019	Added bug 593993 to the "Known Issues" section.

# Introduction

This document provides the following information for FortiSwitch 3.6.10 build: 0430.

- [Supported models on page 5](#)
- [Special notices on page 6](#)
- [Upgrade information on page 11](#)
- [Product integration and support on page 12](#)
- [Resolved issues on page 13](#)
- [Known issues on page 14](#)

See the [Fortinet Document Library](#) for FortiSwitch documentation.

## Supported models

FortiSwitch 3.6.10 supports the following models:

<b>FortiSwitch</b>	FS-108D-POE
	FS-124D
	FS-124D-POE
	FS-224D-POE
	FS-248D-FPOE
	FS-248D-POE

## What's new in 3.6.10

FortiSwitch 3.6.10 is a patch release only. No new features or enhancements have been implemented in this release.

# Special notices

## Supported features for FortiSwitchOS 3.6.10

The following table lists the FortiSwitch features in Release 3.6.10 that are supported on each series of FortiSwitch models. All features are available in Release 3.6.10, unless otherwise stated.

Feature	GUI supported	108D-POE 224D-POE	124D 124D-POE 200 Series
Link aggregation group size (maximum number of ports) (See Note 2.)	✓	8	8
Auto module max speed detection and notification	✓	—	—
IP conflict detection and notification	—	✓	✓
IP-MAC binding	✓	—	—
Static BFD	—	—	—
Hardware-based ECMP	—	—	—
Private VLANs	✓	—	✓
LLDP transmit	—	✓	✓
Loop guard	✓	✓	✓
LAG min-max-bundle	—	✓	✓
sFlow	✓	✓	✓
Storm control	✓	✓	✓
ACL	—	—	✓
Static L3/hardware-based routing	✓	—	✓
Software routing only	✓	✓	—
CPLD software upgrade support for OS	—	—	—

Feature	GUI supported	108D-POE 224D-POE	124D 124D-POE 200 Series
PoE-pre-standard detection (See Note 1.)	✓	✓	✓
VLAN tag by ACL	—	—	✓
ACL redirect to mirror destination as trunk/LAG	—	—	✓
MAC/IP/protocol-based VLAN assignment	✓	✓	✓
802.1x port mode	✓	✓	✓
802.1x MAC-based security mode	✓	✓	✓
User-based (802.1x) VLAN assignment	✓	✓	✓
Virtual wire	✓	—	✓
HTTP REST APIs for configuration and monitoring	—	✓	✓
Split port	—	—	—
IGMP snooping	—	—	✓
Per-port max for learned MACs	—	—	✓
802.1p support, including priority queuing trunk and WRED (release 3.5.1)	—	—	✓
DHCP snooping	—	—	✓
LLDP-MED	—	✓	✓
DHCP relay feature	—	—	✓
Support for switch SNMP OID	—	✓	✓
Access VLANs (See Note 5.)	—	—	✓
802.1x enhancements, including MAB (release 3.5.1)	✓	✓	✓
Multi-stage load balancing (release 3.5.1)	—	—	—

Feature	GUI supported	108D-POE 224D-POE	124D 124D-POE 200 Series
MCLAG (multichassis link aggregation)(release 3.6.0)	—	—	✓ (not on 124D/124D- POE)
Dynamic layer-3 protocols (OSPF, RIP, and VRRP) (release 3.6.0) (See Note 3.)	✓	—	✓ (not on 124D/124D- POE)
Dynamic ARP inspection (release 3.6.0)	—	—	✓
Firmware image rotation (dual-firmware image support) (release 3.6.0)	—	✓ (not on 108D-POE)	✓
TDR (time-domain reflectometer)/cable diagnostics support (release 3.6.0)	✓	—	✓
MAC learning limit (release 3.6.0) (See Note 4.)	—	—	✓
Sticky MAC on switch interfaces (release 3.6.0)	—	—	✓
PoE modes support: first come, first served or priority based (PoE models) (release 3.6.0)	—	✓	✓
ACL: egress mask action support (release 3.6.0)	—	—	✓
Monitor system temperature (threshold configuration and SNMP trap support) (release 3.6.0)	—	✓	✓
'forced-untagged' or 'force-tagged' setting on switch interfaces (release 3.6.0)	—	✓	✓
Selective packet sampling to CPU (useful diagnostic tool) (release 3.6.0)	—	—	✓
Add CLI to show the details of port statistics (release 3.6.0)	—	✓	✓
Display progress (%) during firmware upgrade (release 3.6.0)	✓	✓	✓
STP root guard (release 3.6.2)	—	✓	✓
STP BPDU guard (release 3.6.2)	—	✓	✓
IGMP snooping: static multicast groups (release 3.6.2)	—	—	✓



Feature	GUI supported	108D-POE 224D-POE	124D 124D-POE 200 Series
DHCP snooping: entry limit per port (release 3.6.2)	—	—	✓
Network device detection (release 3.6.2)	—	—	✓
QoS queue counters (releases 3.6.2 and 3.6.3)	—	—	✓
Support of the RADIUS accounting server (release 3.6.3)	—	✓	✓
Support of RADIUS CoA and disconnect messages (release 3.6.3)	—	✓	✓
802.1x authentication: EAP-TLS support (release 3.6.3)	—	✓	✓
DHCP snooping: CLI for DHCP-snooping server database (release 3.6.3)	—	—	✓
Unicast hashing (release 3.6.4)	—	—	✓
STP supported in MCLAGs (release 3.6.4)	—	—	✓ (not on 124D/124D- POE)
QoS marking (release 3.6.4)	—	—	✓
MAB reauthentication disabled (release 3.6.4)	—	✓	✓
Cut-through switching (release 3.6.4)	—	—	—
Control of temperature and PoE alerts (release 3.6.4)	—	✓	✓
IGMP querier (release 3.6.4)	—	—	✓
Configuration of the QSFP low-power mode (release 3.6.4)	—	—	—
Learning limit violation log (release 3.6.4) (See Note 4.)	—	—	✓
Sticky MAC addresses saved to static MAC table (release 3.6.4)	—	—	✓
Enabling packet forwarding to CPU (release 3.6.4)	—	—	✓

## Notes

- PoE features are applicable only to the model numbers with a POE or FPOE suffix.
- 24-port LAG is applicable to 524D, 524\_FPOE, 1024D, and 3032D models. 48-port LAG is applicable to 548D, 548-FPOE, and 1048D models.
- To use the dynamic layer-3 protocols, you must have an advanced features license.

- 
4. The per-VLAN learning limit and per-trunk learning limit are not supported on dual-chip platforms (248 and 448 series).
  5. Access VLANs are not supported on 108D-POE, 224D-POE, or 112D-POE.

# Upgrade information

FortiSwitch 3.6.10 supports upgrading from FortiSwitch 3.5.0 and later.

## Cooperative Security Fabric upgrade

FortiOS 5.4.1 greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1
- FortiClient EMS 1.0.1
- FortiAP 5.4.1
- FortiSwitch 3.4.2

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Framework - Upgrade Guide*
- *FortiOS 5.4.0 to 5.4.1 Upgrade Guide for Managed FortiSwitch Devices*

This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2.

# Product integration and support

## FortiSwitch 3.6.10 support

The following table lists 3.6.10 product integration and support information.

<b>Web browser</b>	<ul style="list-style-type: none"><li>• Microsoft Internet Explorer version 11</li><li>• Mozilla Firefox version 52</li><li>• Google Chrome version 56</li></ul> <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
<b>FortiOS (FortiLink Support)</b>	FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later.

## Resolved issues

The following issues have been fixed in 3.6.10. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
506762	It is difficult to access the switch when an IP camera is connected to port 21.
521950	After a FortiSwitch unit is restarted, FortiLink is not restored when there is a switched virtual interface (SVI) on the FortiSwitch unit, and the mode is DHCP.
541865	The <i>Log &gt; Event Log &gt; System</i> page does not display detailed logs when there are changes made in an admin session.
541871	A managed FortiSwitch unit cannot be reached by SSH when using a public key.
549033	The <code>diagnose sniffer packet</code> command does not work for the split-port configuration.
551173	After enabling SNMP on two 448D switches and connecting them to a network-management app, SNMP crashed.
553368	Using a network-management app caused the SNMP daemon to use more memory.
556389	The <code>show full system certificate local</code> and <code>show full system certificate ca</code> commands increase the memory usage.
567984	When a managed FortiSwitch unit is restarted, the lldp profile configuration for the ports changes from “default” to “default-auto-isl” briefly.

# Known issues

The following known issues have been identified with 3.6.10. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
380239	<p>IGMP-snooped multicast groups are not immediately flushed out of the snooping table when the querier port is shut down.</p> <p><b>Workaround:</b> Upgrade to FortiSwitchOS 6.2.0.</p>
391607	<p>Switch does not send gratuitous ARP for IP conflict when the system boots up and adds a new switch virtual interface (SVI).</p> <p><b>Workaround:</b> Upgrade to FortiSwitchOS 6.2.0.</p>
414972	<p>IGMP snooping might not work correctly when used with the 802.1x dynamic VLAN functionality in the 802.1x MAC-based authentication.</p>
416655	<p>When using DHCP, the IPv6 address cannot be configured. Also, the automatic configuration of the global address does not work.</p> <p><b>Workaround:</b> Upgrade to FortiSwitchOS 6.2.0.</p>
424432	<p>When MCLAG is enabled In FortiLink mode, IGMP reports are not synchronized if the <code>igmps-report-flood</code> and <code>igmps-traffic-flood</code> options are disabled the the FortiLink/ISL/MCLAG trunks.</p> <p><b>Workaround:</b> Upgrade to FortiSwitchOS 6.2.0.</p>
438441	<p>DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANS).</p>
509787	<p>FortiSwitch Cloud is disabled when upgrading FortiSwitch firmware.</p>
510943	<p>When using the cable diagnostics feature on a port (with the <code>diagnose switch physical-ports cable-diag &lt;physical port name&gt; CLI command</code>), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.</p>

Bug ID	Description
535736	<p>If a FortiSwitch firmware image is an even multiple of 1024 bytes, it will not upgrade properly using the default FortiLink upgrade mechanism. The following builds are known to be affected:</p> <p><b>version 3.x</b> build 0415/FSW_124D_POE</p> <p><b>version 6.x</b> build 0039/FSW_1048E build 0043/FSW_124E build 0141/FSW_224D_FPOE build 0052/FSW_548D_FPOE</p> <p><b>Workarounds:</b> Change to HTTPS mode using the following commands:</p> <pre>config switch-controller global   set https-image-push enable end</pre> <p>Alternatively, you can upgrade to FortiOS 6.0.5 or 6.2.0.</p>
593993	<p>When the switch-controller.global.https-image-upgrade is enabled, the FS-108D-POE/FS-224D-POE might fail to upgrade.</p> <p><b>Workaround:</b> Disable https-image-upgrade.</p>



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.